Undersea Optical Cable Network and Cyber Threats

Aarne Hummelholm
Faculty of Information Technology, University of Jyvaskyla, Finland
aarne.hummelholm@elisanet.fi

Abstract: Almost all services and most of the traditional services are totally dependent on the digital environment. Few users are aware of the revolutionary nature of modern technology. We use day-to-day real-time access to existing digital services in our home country or we use social media (Some) to communicate with friends locally or elsewhere in the world. We can communicate with them in real time with text messages or even through real-time video feed. People have the choice of millions of movies to watch anytime, anywhere. Modern communications connect data centers and data networks of different continents together, enabling real-time communications throughout the world. We can order different goods from all over the world, pay invoices electronically and get the goods delivered to our door. Companies use the same channels of communication for daily communications, trading, sending invitations to tender and transferring money through banks in real time. As a result of the developments described above, people and systems produce huge amounts of data which needs to be processed and stored. However, technical solutions for all new service environments are not yet in line with international standards and their connections to telecommunications and service networks are very diverse. Technically outdated solutions and new technologies are used simultaneously. Future information and communication systems need to be designed and adapted to work in this challenging business environment where security threats and cybercrime are constantly present. Each function has its own service and communication needs depending on the user group. These groups include design and maintenance staff, financial management staff, telecom operators, service provider staff, virtual service providers and operators, administrative agents, citizens, manufacturers, banks, etc. To date no other technology apart from submarine cables systems has had such a strategic impact to our society while at the same time remaining so badly understood by the general population. This means that it is also a very tempting target for hackers and state actors. They seek access to the sea cables and networks connecting continents to each other.

Keywords: communication, continents, cybercrime, submarine cables, hackers

1. Introduction

We will look first at how different parts of the world are currently connected to each other by submarine optical cables, figure 1.

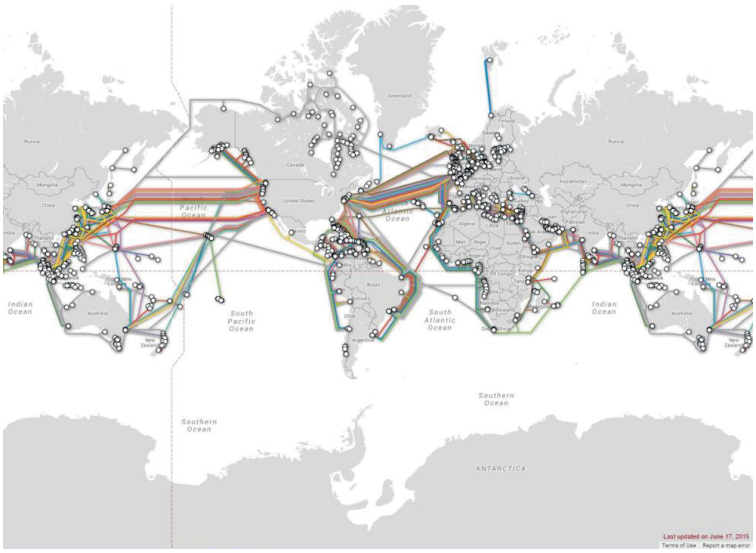

Figure 1: Map of the Worldwide Undersea Submarine Cable Network (Reddit (2017)).

These cables are concentrated in the southernmost seas of the globe, and the terminals for submarine optical cables are located in areas where it is relatively easy to build cable endpoints, including cable communication and energy systems. Each country has its own fiber network that connects cities and the countryside to each other.

Currently submarine optical cable route between Asia and Europe is long. It is very possible that one way or another an undersea submarine optical cable system will break down. Terrorists can deliberately damage them, cyber attackers can penetrate them, natural disasters are a risk and so on. These and many other risk factors are

a good reason for us to design a new submarine optical cable route between Asia and Europe in order to ensure secure communication links between these areas. Figure 2 is a general overview of the Artic Optical Cable Systems, which combines different regions of Europe, the western parts of Russia, the Siberian Russian regions, areas in the Russian Far East, smart cities in Japan and the border areas of China.

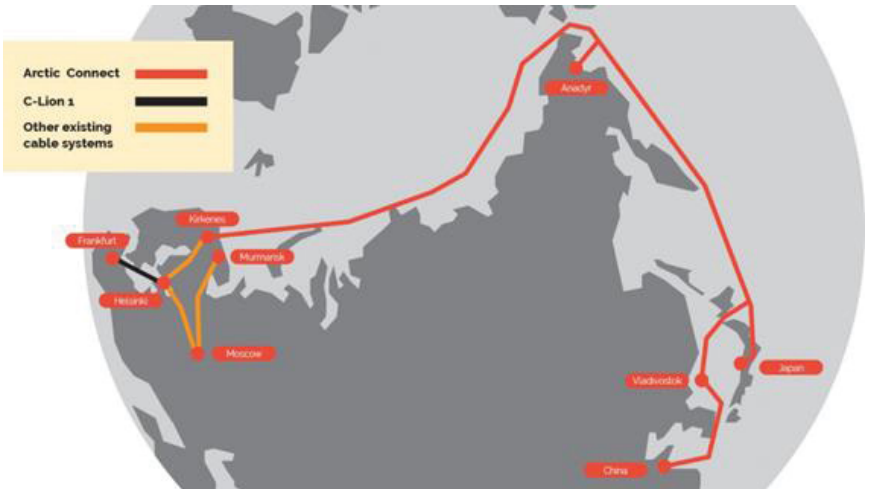

Figure 2: The Artic connect cable system (Jukka-Pekka Joensuu (2018)).

A lot of communication capacity and many new contact points will be needed in the future in order to satisfy the data transfer needs of users, businesses organizations and governments in these areas. These areas require proper and reliable communication links to be able to communicate and use the services offered by the rest of the world. Regional development and joint operations in these northern areas require there links. This new connection gives people in the area real-time access to existing digital services in their home country and they can use it to communicate with their friends either locally or anywhere else in the world.

2. Chapter 1: Objective and organization of the paper

The research question is: whether is it possible to rely on submarine optical cable systems for communication between different continents?

This study seeks a model to facilitate threat assessments and the comparison of threats and to facilitate the threats analysis in these types of ecosystems. In view of the fact that the plan is focused on ocean environments, particularly in the Arctic, in addition to the technical design criteria, also different types of threats such as natural threats, accidents, as well as terrorists and cyber-attack threats must be taken into account. The results obtained through the model will aim to facilitate the design and implementation of architectural solutions. The implemented model can help in improving the assessing the threat scenarios for future submarine optical cables system environments and their impact probabilities. The study utilizes the operating environment as introduced in Figure 2, where different part of continental services and infrastructure are grouped together. Threat research can be done by submarine optical cable in different segments and assess the types of threats to those segments. The political and commercial aspects of the Arctic region have not been included. The continent`s telecommunication networks, submarine optical communications networks and data centers with their services are effectively one entity, through which all future services will be implemented; and, in the future, they will also be working together both in the different continents and between them. The integration described above is accelerating at all levels of activity, in each region and al segments both horizontally and vertically. The nature of these environments will further complicate doing threat estimates of this kind of ecosystems.

Chapter 2 presents the ecosystems and future operating environments of the telecommunication networks, data centers and the submarine optical communications networks a general level. Chapter 3 describes the natural threats, accidental threats, cyber-threats and dependency analyses which are used to make a threat analysis of the submarine optical communications networks and network infrastructures and the services it provides. Chapter 4 deals with the making and modelling of threat analyses, and Chapter 5 describes the conclusions, solution model for security and future work.

3. Chapter 2: Description of the future operating environment and technology

In the smart societies of the future, the amount of information will increase exponentially, as people use their smart devices not only to send messages but also to send real-time videos, to watch movies, and so on. Everything will be done in real time. Therefore, a very large amount of storage space will be required, which in turn means more data centers. Retrieving data from different networks also involves high real-time requirements, so data centers will also need to be as close as possible to the users. Figure 3 shows the smart societies of the future; a high-level architectural description of the smart societies, with large and small data centers, close to the users. Similar structures will be developed in both Europe and in Asia. These European and Asian Smart societies of the future will be connected to each other by a new route, when the Artic Optical Cable System is installed. The estimated of the incoming connection length of the Artic Optical Cable`s route is about 18.000-20.000 km (Figure 2). This sets a number of requirements both for the design and the implementation of this submarine optical cable system. Overview of the Artic connect cable system are seen in Figure 4, which was examined.

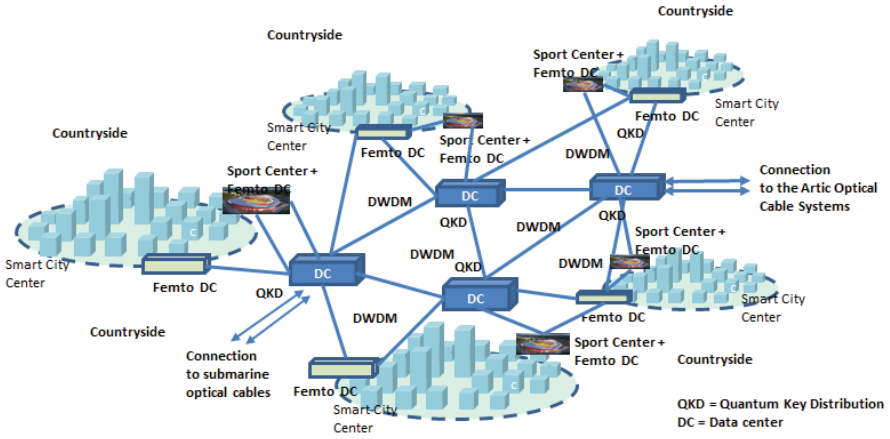

Figure 3: Smart Cities in the future environment, top level principle.

The Artic optical cable route will also be of interest to hackers, terrorists, cyber attackers and state actors, as there is going to be a lot of information crossing from Europe to Asia and vice versa.

Because of the importance and the length of the link, the technical values and requirements that affect the design of the system must be investigated and the result utilized in both the design and the maintenance of the system. When we perform system deployment measurements, those values can be used later to detect the smallest changes in the system and identify any attempts attacking the system. These problems or defects may be caused by natural forces, construction works at sea, terrorists or cyber attackers. All such phenomena cause lesser or greater changes in the measured values associated with the operation of the system. Unfortunately, not all situations can be obtained from identifiable numerical data that can be detected by management and control devices, for example, the tapping of submarine optical cable results in less than a 2% loss of optical signal power and it is thus not so easily correctly detected by using existing technologies. Consequently, even the smallest deviations must be reviewed and analysed. For this reason, we must identify the factors affecting fiber quality that result from the properties of the fibres themselves. This is important to know and take into consideration because it affects the construction of a connection in a number of ways, such as the wavelength and bandwidths supported by the fibres, distance between optical amplifiers from each other, the optical signal levels to be used, etc. As this is also a long-term investment and the submarine optical cable may be in use for more than 25 years, the evolution of technology must also be taken into consideration, in order to anticipate early and timely updates and changes to the systems and equipment. In addition, when transmission speeds are increased in the wavelength by the fibres, there will still be a few boundaries that we can no longer exceed with the current technology. These are the physical limits of single-mode fiber (SMF) and two other limits of optical communications – the Fiber-launched power limit and the Non-linear Shannon limit (Yutaka Miyamoto (2017)).

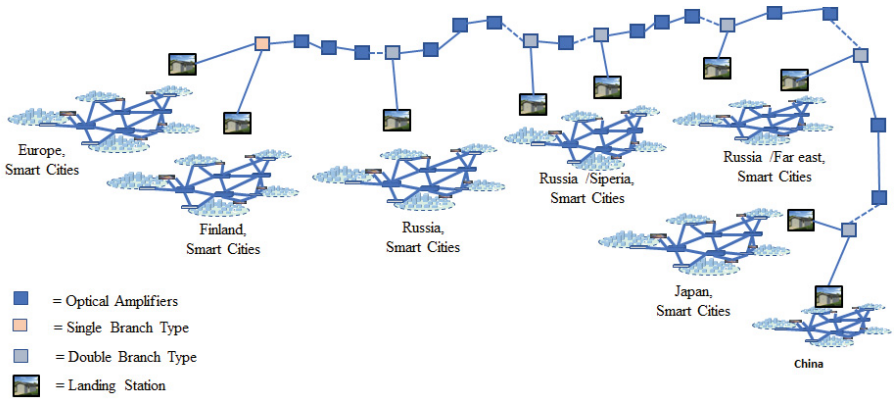

Figure 4: Overview of the Artic connect cable system.

4. The evolution of technology

As the life cycle of the optical cable system we must understand at least in part, the technical evolution that will occurs in optical telecommunication technology and how that will affect these long connections. The optical channel capacity cannot be increased indefinitely, despite the wide optical bandwidth available in the optical range. We can calculate the optical channel capacity that will be able to be achieved (Chesnoy Jose (2016)). We can look at Shannon's definition of the upper limit for transmission capacity (or spectrum efficiency) that can be transported in transport channel as $C = B \log (1 + SNR)$, with C being the capacity in bit/s, B the bandwidth in Hz, and SNR being the signal-to noise- ratio. We can also define the single-sided optical noise power spectral density as $S_n = hv/2$, where $h = 6.63 \times 10^{-34}$ Js is the Planck value, hv is the proton energy 10^{-19}J, and the minimum average optical noise power $P_N = (hv/2)\, B_0$ is proportional to the bandwidth.

Therefore, the optical channel capacity, treated in terms of the optical field, is:

$$C = B_0 \mathrm{Log}_2 (1 + 2P_s / hvB_0) \quad (1)$$

We must also take into account the features of these optical submarine optical cables systems parameters in practical networks to get more accurate information about the functions of the existing system so that we can detect possible intrusion attempts. Since more capacity is needed per fiber pair, new optical signal band, L-band is introduced. The C and L bands form the basic band of future long-distance optical networks ITU-T Manual (2009)). This provides a challenge to network designers to find an optical amplifier with enough bandwidth. In C-band, there are 80 optical channel and also in L-band has 80 optical channels. If we transmit 100 Gbit/s through one wavelength, this means, for examples, that we would have 80 X 100 Gbit/s capacity in use in this kind of network.

5. Long distance submarine optical systems

By 2015 there was a mature product had the capacity of 100 Gbit/s per optical wavelength. Since then ongoing development has continued to find new solutions aimed at increasing wavelength capacity per optical wavelength. As a result of this development, capacities of 200 Mbit/s and 400 Mbit/s are now available. In order to obtain transmission rates 100 Mbit/s or more in submarine optical cables, it would be necessary to install optical amplifiers at about 50 km intervals. This distribution would provide sufficient quality of service across continents.

6. The primary principles of the installation

18.000 km long submarine optical cable system will be installed In the Artic region (Figure 2). There will be few branching points with connections to the continent (figure4). In Figure 5 Data Center NMS means Network Management System, and TLTE means Terrestrial Line Terminal Equipment. Cable Landing Station NMS means Network Management System, LME means Line Monitoring Equipment, PFE means Power Feed Equipment, SLTE means Submarine Line Terminal Equipment. Each cable landing station will be built in the same way. Difference between them will be only how the submarine's optical cables can be brought to the station of course and it depends on the beach area.

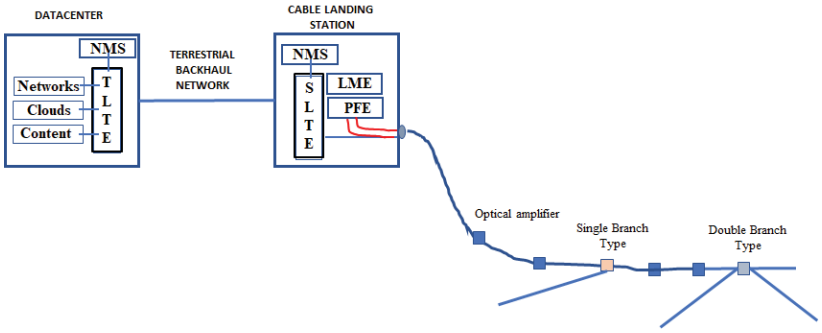

Figure 5: Subsea Optical Cable System Architecture with Cable Landing Station and Data Center

The main reason for the distance between optical amplifiers is only 50 km is due to the dispersions and non-linear properties of optical cables, the characteristics of the optical amplifiers, noise levels and the characteristics of the fiber. As the modulation techniques of optical data transfer become more complex, we must design systems even more carefully. The distance between the amplifiers is optimized based on the usability and quality of the services. Performance and cost optimization are expressed in terms of cost efficiency €/bitti/hz. These whole systems also need electrical energy. Energy input to the system can be made of one or more earth points, taking the energy supply protection into account in case of a damage in cable systems.

7. Designing submarine optical cable systems

In order to achieve the required usability and quality requirements for very long optical undersea cable connections, the following factors must be taken into account.

Factors affecting fiber connections quality

7.1 Attenuation

Attenuation values vary between different wavelength bands and should be smallest in the 1550 nm band, where it is about 0.2 db/km or less.

7.2 Dispersions

There is tree type of dispersions; Rayleigh Scattering, Chromatic Dispersion and Polarization Mode Dispersion (PMD), which we must take into account. Optical Signal-to-Noise Ratio, OSNR, must also be take into account as it limits the distance between optical amplifiers.

7.3 Impact of non-linearity

Optical fibers also have nonlinear characteristic like; self-phase modulation (SPM), cross-phase modulation (XPM), four-wave mixing (FWM), stimulated Raman scattering (SRS), and stimulated Brillouin scattering (SBS). Those characteristics must be given special attention as the phenomena they cause may be the result of a cyber attacker's action that were not detected by the normal management and control systems of the submarine optical cables.

8. Chapter 3: Natural threats, accidental threats and cyber threats

In addition to the technical design criteria, we also need to take into account the various type of threats that will be encountered such as natural threats, accidental threats and cyber or malicious threats. These threats can contribute to prolonging cable routes or partial routes or even altering the originally planned routes. Natural threats include threats such as sharks, earthquakes, landslides, volcanic, eruptions, tsunamis, icebergs, sea currents, storm winds and so on. Accidental threats can be caused by everyday work at sea, such as fishing, dragging an anchor, dredging etc. and can damage submarine optical cables, threatening their level of performance. We also need to look at other potential threats since the submarine optical cable routes are long. Many countries have the ability to join (tap) fiber optic cables in order to collect the information being transmitted there in. In every situation, we must always be on outlook for opportunities to hack into or launch cyber-attacks on submarine optical cables – whether this be “tapping” the lines or other methods such as side channel attacks or side channel spying.

The type of undersea cables types chosen depends on the depth of the sea and the vicinity of the coast in the areas where the above-mentioned threats exist, and the threats are realized. If we consider at cyber attackers` opportunities to join to the optical cable, it would be easiest to penetrate the cable exactly where the cable armoring layers are thinnest. This also means that the attacker must be able to operate deep below the sea level. In practice, only a few large states have the capabilities to do this. When considering this planned undersea optical cable system, with a length of 18,000 km, cyber attackers will be able to connect to undersea optical cables after each optical amplifier, which are deep underwater area. Next, we can consider a submarine optical cable system, based on ITU-T Recommendation G.709, G.971 and G 977. It is divided into a land section, an underwater section, and a second part of the land section. The underwater section has the necessary branching equipment. When we have a 18,000 km long submarine optical cable system in use, we also need Power Feed Equipment for our submarine optical cable systems.

We also need different types of OTDR (Optical Time Domain Reflectometers) to certify the performance of new fiber optics links and detect problems in existing fiber links. It is now possible to use measurement system like COTDR, Coherent Optical Time Domain Reflectometry, for high capacity systems. It is very important to use COTDR, because in 18.000 km submarine optical cable systems we would use different types of fiber cables for compensating dispersion phenomena. This also means that there is very much cable branching and continued points, so it is very difficult to find the smallest deviations in the parameters. It`s management and control systems are most critical systems. To identify security challenges in long distance optical cable systems, we must consider Optical Transport Network (OTN) framing and rates, Figure 6, and Optical Transport Network (OTN), OSI layer model, Figure7. Currently, no encryption technology is in use for optical signals. Figure 6 shows the OTN Optical Transport Network (ITU-T, G.709), where the client signal is seen and how the header areas of the different layers are placed in relation to the client signal. Figure 7 can be seen more precisely portraying that what information a cyber attacker could access and use if we do not encrypt these signals. For example, they can change the ROADM, the Reconfigurable Optical Add-Drop Multiplexer, routing in whatever way they want, and either disrupt traffic or drive traffic to a desired connection point, for analysis.

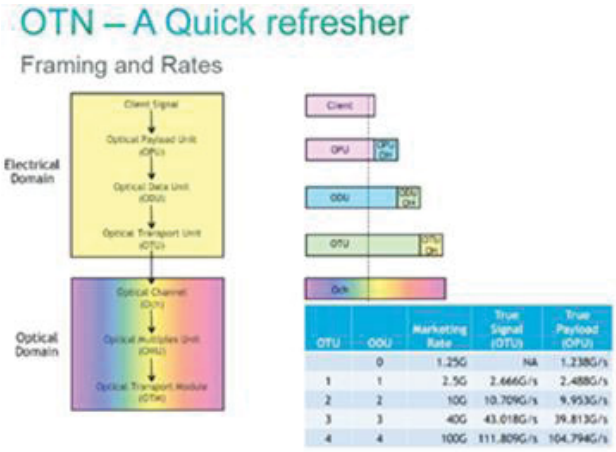

Figure 6: OTN Optical Transport Network, framing and rates, (ITU-T, G.709).

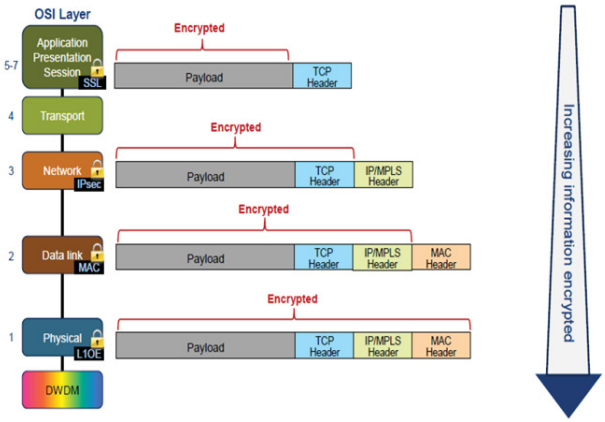

Figure 7: OTN Optical Transport Network, OSI layer and engryption (ITU-T, G.709).

From Table 1 we can see upper level conceptual submarine cable segments` threat matrix which we need to take it account when we are designing and developing undersea submarine optical cables systems.

Table 1: Upper level conceptual threat matrix for submarine cable segment, on "Threats to Undersea Cable Communications, September 28, 2017".

Submarine Cable Segment Threat	Land and Beach Area (Seg.1)	Near Shore Area ~50 m (Seg.2)	Off Shore Area ~ 50 – 100 m (Seg.3)	Continental Shelf ~ 100 – 200 m (Seg.4)	Deep Sea ~ 200 m + (Seg.5)
Natural Threats					
Sharks					
Earthquake					
Landslide					
Volcano					
Tsunami					
Iceberg					
Ocean currents					
Accidental Threats					
Fishing					
Anchor dragging					
Dredging					
Malicious and undersea warfare					
Cyber Attacks					
Vandalism					
Activists					
Theft					
Terrorist					
State-actors					
Undersea warfare					

Threat impact level depicted in colours: Green = Low; Yellow = Medium; Red = High

9. Chapter 4: The making and modelling of a threat analysis.

Table 1 illustrates the upper level conceptual threat matrix for submarine cable segments, based on threats to submarine cable communications. We should also note that cyber attackers, hackers and terrorists can use artificial intelligence to enable them to search from vulnerabilities in submarine optical cable systems through which they can penetrate the systems and its services. After doing so they should have the ability to attack Data Centers, different continents. There are many ways that cyber attackers can get inside a submarine optical cables system and to gain access its managements and control systems.

In figure 8 is presented threat probability tree model in the Artic connect cable system, which is used in threat model. Table 1 is divided according to the depth of the submarine optical cable system into different segments and those segments are still divided into different types of categories of threats. Probability of a threat in every segment we can calculate it threat based on information we get from international research reports, from The European Space Agency (ESA), from the Arctic statistics, from sensors and sonars, news concerning on natural or animal cases, accident or injury cases, cyber-attacks etc. how many times they occur and in what areas and at what time of year. This threat probability calculation can be done for the full length of the cable system or just a part of the cable system. In situational picture we need also information from the power supply station`s status.

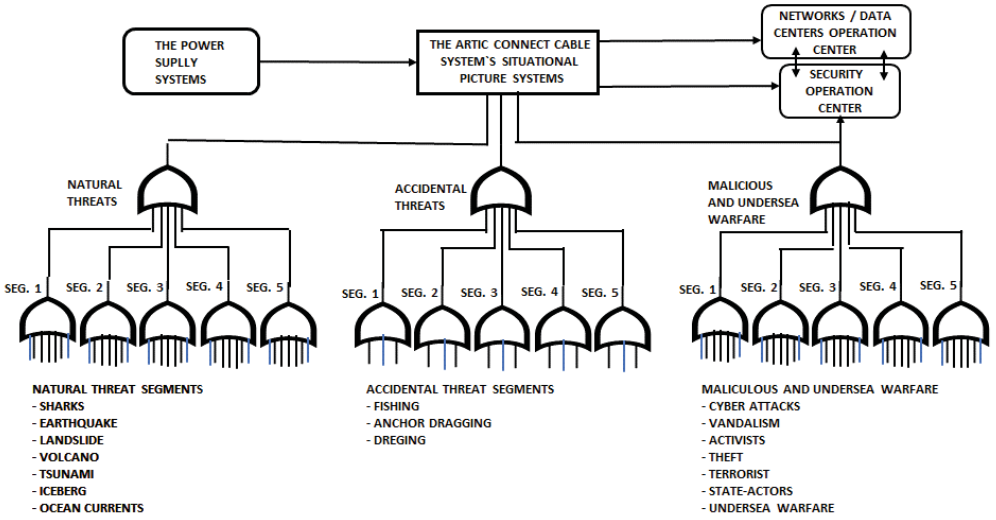

Figure 8: Threat tree model for the Artic connect cable system, example.

Table 2: Meaning of notations

Action	Examples	Notation
Threats or attack	Sudden event, Accident, Tapping, Eavesdropping, Sniffing, Scanning, …,	A
Detection	Alarm information, systems management information, international information, …,	D
Countermeasure	Analysing of threats and vulnerabilities and to repairing, safeguards put in place, …,	M

Threats (P(t)), probabilistic treats or attacks happen.

$P1_{S1\ldots7}$(t) = $P1_{A1\ldots7}$(t)(1 – $p1_{D1\ldots7}$(t))(1 - $p1_{M1\ldots7}$(t)), to 7 different types natural threats. (1)

$P2_{S1\ldots3}$(t) = $P2_{A1\ldots3}$(t)(1 - p2$_{D1\ldots3}$(t) (1 – $p2_{M1\ldots7}$(t)), to 3 different types accidental threats. (2)

$P3_{S1\ldots7}$(t) = $P3_{A1\ldots7}$(t)(1 – $p3_{D1\ldots7}$(t)) (1 – $p3_{M1\ldots7}$(t)), to 7 different types malicious and undersea warfare. (3)

$P1_{S1\ldots7}$(t) = [($P1_{S1}$(t)) + (P1$_{s2}$(t)) + … + ($P1_{s7}$(t))], information to the situational picture systems. (4)

$P2_{S1\ldots3}$(t) = [($P2_{S1}$(t)) + (P2$_{s2}$(t)) + ($P2_{s3}$(t))], information to the situational picture systems. (5)

$P3_{S1\ldots7}$(t) = [($P3_{S1}$(t)) + (P3$_{s2}$(t)) + … + ($P3_{s7}$(t))], information to the situational picture systems. (6)

In figure 8, the situational picture system is for every threat-type own icon, which is telling situation in that segment in the Arctic connect cable system in every part of it. Information from situational system is also send to the security operation center and also network management centers and data center`s management systems. That situational picture systems should be in different areas of the Arctic connect cable system for network operators and for service provider their own, because of response time must be fast enough to start for example, in rescue operations. The Arctic connect cable system whole situational picture information must be also in the cable operator`s operation center.

The land and beach areas of submarine optical cables systems are the easiest for attackers to penetrate. When using large capacity systems in undersea environment, and new types of modulation technology in those systems, the best possible cable tapping points for cyber attackers are after every optical amplifier in deep underwater area. This offers them various opportunities to obtain large amount of information from different companies, organizations and governments. In this situation cyber-attackers and hackers can obtain IP addresses from these companies`, organizations` and governments` and either make DDOS (Distributed Denial of Service attack) attacks against them or use different types ransomware or malware attacks against them. Ransomware attacks are typically carried out by using a Trojan, entering a system through, for example, a vulnerability in a

network service. One possible cyber-attack model is an advanced persistent threat (APT), which is a targeted cyberattack in which an intruder gains access to a network and remains there undetected for a long time. APT attacks typically target organizations such as national defense, manufacturing, and the financial industry, and also companies that deal with high-value information, military plans, and other data from governments and enterprise organizations. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.

Figures 6 and 7 illustrate, if attackers gain access to the submarine optical cable system and there is not encryption system in use, they will also have access to the its management system and thus have the ability to use it to do whatever they want and what suits their purposes. We also need to take into account the power supply system, so that we can be certain that it does not have any vulnerabilities that an attacker can take advantage of in order to attack to our systems.

Considering Figures 3 and 4, Communications Networks in The Future, between different smart cities, we must also look at communications inside the cities, where there are many challenges, presented by the operating environment and heterogeneous telecommunication networks. New devices and systems are seamlessly interconnected there. These systems have expanded into homes, building automation systems, cars and various control and energy systems and people are now using their personal smart devices everywhere. These smart city systems also need their own applications, and their information is stored in a Data Center, shown in Figure 3 and 4. This also means that hackers, terrorists and cyber attackers have many opportunities to find vulnerabilities in this environment, and to attack these Smart City's applications and services. This in turn allows hackers and cyber attackers to attack services and service systems, even on other continents because the Data Center are interconnected.

10. Chapter 5: Conclusions, solution model for security and future work

The system to be built is technically very complicated and will needed many new technical solutions to meet the required transmission rates and usability and quality parameters. This places considerable demands on the management and control of the system as well as on the organization of its maintenance. Changes in social structures take place very quickly and will also affect the implementations and operating models and structures, as well as people's everyday lives and working environments. The current powerful digitalization trend increases the range of services offered and facilitates their easier use. These developments also have a strong impact on the service chains of the provided services, including subcontractors and their subcontracting chains, hardware solutions, service providers and operating models for every part of the service chain on every continent.

Today and in the future modern communications connect data centers and data networks on different continents, enabling real-time communication throughout the world. This type of communications is made possible by undersea optical cable systems, which we use for daily communications. Because submarine cables systems have had such a large strategic impact to our society, they are also a very interesting target for hackers, cyber attackers, terrorist and state actors. They seek to gain access to the information that goes through the networks of these continents which are connected to each other with sea cables. For example, we need to be aware of the possibility of cyber attackers being able to connect to optical fibers, they have the option to change the ROADM routes, which can lead to the communication or disruption of traffic between the entire continent. When considering the cyber security in systems design, we must take into account the upcoming technologies, which means there are more challenges ahead of us. In addition, changes in the cable technology due to dispersion phenomena make their own challenges in detecting intrusion into the cable. We have to be really careful about the design.

11. A solution model for security

Since this new submarine optical cable system (Figure 2), is so long and it is impossible to detect or identify all of the potential attacks against it, it is recommended that an end-to-end encryption system on each wavelength individually at the lowest layer, be put in place. Figure 7 illustrates why this is advisable, as we can see the optical traffic network, the OSI layer and what effect encryption this layer have. When we implemented encryption on the lowest layer, we protect our entire communications systems against various types of attacks. There are currently encryption systems of this type in use, but the capacity to be used may present challenges to those devices and systems. The Quantum encryption system is also currently operational use however such an environment would present challenges regarding the renewal of encryption keys in each optical amplifier.

Individual smart devices are also tested with different types of VPN-encryption`s concepts, but that research is still ongoing although it is hoped that the results will be ready by next year.

12. Future work

Because the Artic connect cable system is a critical system that will be used by many countries, organizations and people for their own purposes, it is essential to study the key issues affecting its functioning. With regard to cyber security, the use of Artificial Intelligence (AI) needs to be investigated and its potential to protect submarine optical cable systems needs to be clarified in order to better protect against malware and cyber-attack.

- With regard to cyber security, the use of Artificial Intelligence (AI) use needs to be investigated, and its potential to protect submarine optical cable systems needs to be clarified in order to better protect against malware and cyber-attacks.
- The possible use of COTDR should be investigated as it is used for searching for faults and can also be used to detect the tapping of cable connections.
- We must study a variety of protection mechanism for submarine optical cables system`s because it is an extremely important fiber optic connection between different continents.
- One study area would be different encryption systems, such as quantum encryption or Layer 1 - 2 encryption systems.

References

Chesney Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016.

Covernance for Cyber Security and Resilience in the Arctic, Advanced Research Workshop 27 – 30 January 2019, Rovaniemi, Finland.

Davenport Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24Cath. U. J. L. & Tech (2015). Available at: http://scholarship.law.edu/jlt/vol24/iss1/4..

ITU-T, Spectral grids for WDM applications: DWDM frequency grid, G.977 (01/2015)

ITU-T, G.709/Y.1331, Interfaces for the optical transport network, 6/2016.

ITU-T, G.971, General features of optical fibre submarine cable systems, 11/2016

ITU-T, Manual 2009, Optical fibres, cables and systems.

Jukka-Pekka Joensuu, Navigating the Arctic, 13 th February 2018, http://asia.blog.terrapinn.com/submarine-networks/2018/02/13/navigating-the-arctic/..

Reddit, Map Of Underwater Cables That Supply The Worlds Internet, 30 September 2017, www.reddit.com/r/MapPorn/comments/73ekox/map_of_underwater_cables_that_supply_the_worlds/

Threats to Undersea Cable Communications, September 28, 2017, PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM.

Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei, Submarine Optical Cable Engineering, Elcevier Inc. 2018.

Yutaka Miyamoto, Ryutaro Kawawura, Space Division Multiplexing Optical Transmission Technology to support the Evolution of High-capacity Optical Transport Network, June 2017.

disaster area scenarios and for rescue efforts. Thaddeus joined the University of Chester in 2015 to develop and deliver the University's new Cybersecurity programme and research.

Eric Filiol is the head of (C+V)O research lab at ESIEA, France and senior consultant in offensive cybersecurity and intelligence. He spent 22 years in the French Army (Infantry/Marine Corps). He holds an Engineer diploma in Cryptology, a PhD in applied mathematics and computer science and a Habilitation Thesis in Computer Science. He is graduated from NATO in InfoOps. He is the Editor-in-chief of the Journal in Computer Virology. He has been a speaker at international security events including Black Hat, CCC, CanSecWest, PacSec, Hack.lu, Brucon, H2HC…

Nathaniel Flack is pursuing a MS in Cyberspace Operations at the Air Force Institute of Technology in Ohio. He received his BS in Computer Engineering from Cedarville University in Cedarville, Ohio in 2012. His main research areas are cyber education, multi-domain operations, and serious games.

Noran Shafik Fouad is a doctoral researcher in international relations at the University of Sussex, and a recipient of the university's Chancellor International Research Scholarship. Her research examines the peculiarities of digital information and its implications on cybersecurity policy and theory, with a particular focus on the US as a case study.

Saïd Haddad, Ph.D in Political science (René Descartes University, Paris), is Senior lecturer in Sociology and member of the research team, Conflits in Mutation of the Saint-Cyr Research Center at the Saint-Cyr Military Academy, France. His current research focuses on the construction of cyber as a French national priority and the sociology of "cyber warriors".

Gerhard Henselmann, Dipl.-Ing. MBA, graduated Flighttest-Engineer was educated in Aerospace Engineering at Technical University of Munich/Germany and is working over 35 years in aerospace with expert experience in testing, flighttesting of airborne military platforms and has a wide experience in avionics, electronic warfare and self-defence of military platforms. He started his PhD studies in summer 2016 at the University of Jyväskylä on Cyber Security.

Aarne Hummelholm graduated from Helsinki University of Technology in 2000. Since then he has been involved in the design, development of architectures` of authorities` telecommunications networks and information systems. Key themes in his work have been critical service availability, cyber security and preparedness issues. In 2017 he started his doctoral dissertations at the University of Jyväskylä.

Gazmend Huskaj is a PhD candidate in Cyber Operations at the Swedish Defence University. He received his MSc in Information Security from Stockholm University in 2015 as a distinguished graduate. Previously, he was Director Intelligence in the Swedish Armed Forces focusing on cyber-related issues. He is also a ISACA Certified Information Security Manager (CISM).

Ion A. Iftimie is a Doctoral Candidate in Vienna, Austria. Previously, he served as the Deputy Chief for Information Operations at the United States Cyber Command. He graduated from top defense colleges in the United States, Germany, and Sweden, and is an alumnus of the Harvard Kennedy School Executive Program in Cybersecurity Policies.

Eduardo Arthur Izycki is a Student of Master in International Relations by the University of Brasília (UnB) and public servant. Eduardo Izycki worked on developing solutions for risk assessments in the cycle of major events in Brazil (2012-2016). He currently works in the Critical Infrastructure Protection Coordination of the Brazilian Institutional Security Office (GSI).

Margarita Jaitner is an analyst at the Swedish Defense Research Agency. She received her MSSc in Societal Risk Management from Karlstad University Sweden. She has authored several academic publications within the area of information warfare in cyberspace, hybrid warfare and other policy-related research within cyber security.

Dr. Victor Jaquire has been within the field of cyber and information security for over 20 years within Government and the Private sector focusing on strategy, performance management and operations. He holds